We claim:

[c1] A method for providing secure network communication, comprising:

providing an intelligent network interface between a network and each device on the network;

encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces; and

centrally managing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network with a central management console.

[c2] The method of claim [c1], further comprising each intelligent network interface providing protocol translation based on servlets provided by said CMC.

[c3] The method of claim [c3], wherein said protocol translation is selected from the any two protocols within a single layer of an ISO 7 layer protocol stack.

[c4] The method of claim [c2], further comprising said CMC dynamically distributing proxy servlets to intelligent network interfaces based on distinguished name.

[c5] The method of claim [c2], further comprising said CMC dynamically distributing servlets to intelligent network interfaces based on distinguished name, said servlets selected from the group consisting of single sign-on servlets, distinguished name firewall servlets, auditing servlets, policy enforeement servlets, and web-filtering servlets.

[c6] The method of claim [c2], further comprising said CMC dynamically distributing servlets to intelligent network interfaces based on device, said servlets selected from the group consisting of fault tolerance automatic rollover servlets, gateway intrusion detection servlets, multi-level firewall servlets, machine diagnostics servlets, virus scanning servlets, and security patching servlets.

[c7] The method of claim [c1], further comprising:

a first intelligent network interface associated with a first client sending a request to the central management console (CMC) with the identifying information about a connection that the first client wishes to send to a second client, said information including protocol, distinguished name, service, and header information;

said CMC reviewing said connection against a network policy and determining denial or allowance of said connection and, upon allowance, further determining encryption algorithim, authentication required, keys for the connection, if the connection should be redirected to another device, and if the connection needs to be translated;

said CMC sending a connection determination, including encryption and authentication algroithim(s), key(s), and any translation servlets required to said first intelligent network interface;

said first intelligent network interface initiating said connection with a second intelligent network interface associated with said second client by sending

encrypted connection information;

said second intelligent network interface querying said CMC with said encrypted connection information received from said first intelligent network interface, including a Security Paramaters Index (SPI) for said connection that uniquely identifies said connection between said first and second intelligent network interfaces.

[c8] The method of claim [c2], wherein said authentication is selected from the group consisting of username/password, biometric inputs, smart cards, tokens, and combinations thereof.

[c9] The method of claim [c1], further comprising providing a plurality of CMCs on said network in a hierarchical configuration.

[c10] The method for providing distinguished name single sign-on for users of host devices on a network comprising:

providing an intelligent network interface between a network and each device on the network;

providing a central management console (CMC) on said network;

a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device;

the first intelligent network interface verifying the user's authentication with the CMC such that when said user requests services from a second device:

the first intelligent network interface requests communication with said second device based on distinguished name;

a second intelligent network interface associated with said second device queries the CMC for permission and user authentication for the second device based on distinguished name; and

the CMC provides user authentication information based on distinguished name to said second intelligent network interface to allow said second intelligent network interface to log the user into the second device.

[c11] A system for providing secure network communication, comprising:

a network;

a plurality of host devices connected to said network;

an intelligent network interface between each host device and said network;

means on each intelligent network interface for encrypting and decrypting critical data transmissions over the network; and

at least one central management console for providing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network.

[c12] The system of claim [c11], wherein each intelligent network interface further

comprises:

a CPU;

memory;

an I/O interface for the network; and

a second I/O interface for the host device.

[c13] The system of claim [c12], wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI cards, PCMCIA cards, rapid I/O-high bandwidth cards, and standalone devices.

[c14] The system of claim [c12], wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI NIC cards, PCMCIA NIC cards, rapid I/O-high bandwidth NIC cards, and standalone devices with an Ethernet second I/O interface.

[c15] The system of claim [c12], wherein each intelligent network interface further comprises a serial line authentication port.

[c16] The system of claim [c15], wherein said serial line authentication port is a USB port.

[c17] The system of claim [c12], wherein said intelligent network interface further comprises parallel port authentication port.

[c18] The system of claim [c12], wherein said memory consists of flash memory for

storing an OS and dynamic memory for applications.

[c19] The system of claim [c12], wherein said memory consists of a hard drive for storing an OS and applications and random access memory for running said OS and applications.

[c20] The system of claim [c12], wherein said intelligent network interfaces have an OS that is distinct from said host devices.

[c21] The system of claim [c12], further comprising:

an encryption accelerator on a field programmable gate array (FPGA) on said intelligent network interface.

[c22] The system of claim [c11], further comprising:

a set of dynamically distributable code fragments stored on said CMC for distribution to said intelligent network interfaces; and

means on said intelligent network interfaces for using said code fragments to provide functions selected from the group consisting of: authentication, protocol translations, single sign-on, multi-level firewalling, distinguished-name based firewalling, centralized user management, machine diagnostics, proxying, fault tolerance, centralized patching, web filtering, virus scanning, auditing, and gateway intrusion detection.

[c23] A system for providing secure network communication, comprising:

a network;

a plurality of host devices connected to said network;

an intelligent network interface between each host device and said network;

at least one central management console for dynamically distributing security agent servlets to said intelligent network interfaces; and

means on each intelligent network interface for running said security agent servlets.

[c24] The system of claim [c23], wherein each intelligent network interface further comprises:

a CPU;

memory;

an I/O interface for the network; and

a second I/O interface for the host device.

[c25] The system of claim [c24], wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI cards, PCMCIA cards, rapid I/O - high bandwidth cards, and standalone devices.

[c26] The system of claim [c24], wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI NIC cards,

PCMCIA NIC cards, rapid I/O - high bandwidth NIC cards, and standalone devices with an Ethernet second I/O interface.

[c27] The system of claim [c24], wherein each intelligent network interface further comprises a serial line authentication port.

[c28] The system of claim [c27], wherein said serial line authentication port is a USB port.

[c29] The system of claim [c24], wherein said intelligent network interface further comprises a parallel port authentication port.

[c30] The system of claim [c24], wherein said memory consists of flash memory for storing an OS and dynamic memory for applications.

[c31] The system of claim [c24], wherein said memory consists of a hard drive for storing an OS and applications and random access memory for running said OS and applications.

[c32] The system of claim [c24], wherein said intelligent network interfaces have an OS that is distinct from said host devices.

[c33] The system of claim [c23], wherein said dynamically distributed security agent servlets include means to provide functions selected from the group consisting of: encryption, authentication, protocol translations, single sign-on, multi-level firewalling, distinguished-name based firewalling, centralized user management, machine diagnostics, proxying, fault tolerance, centralized patching, web filtering,

virus scanning, auditing, and gateway intrusion detection.

[c34] The system of claim [c33], further comprising an encryption accelerator on a field programmable gate array (FPGA) on said intelligent network interface.

[c35] A method for firewalling based on distinguished name for users of host devices on a network comprising:

providing an intelligent network interface between a network and each device on the network;

providing a central management console (CMC) on said network;

a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device;

the first intelligent network interface verifying the user's authentication with the CMC; and

the CMC dynamically distributing a firewall servlet to said intelligent network interface based on said distinguished name.

[c36] A method of providing non-host integrated fault tolerance for hosts on a network, comprising:

providing an intelligent network interface between a network and each host on the network;

providing a central management console (CMC) on said network;

said CMC dynamically distributing fault tolerance servlets to said hosts such that, upon a failure of a first host, a first intelligent network interface between said network and said first host redirects packets to a second host on said network without any intervention from said first or second host.